

Application No. 09/675,069

Response to Office Action dated 11/04/2004

IN THE CLAIMS:

Please amend the indicated claims as follows:

1. (Currently Amended) A method for executing an algorithm for decrypting data, comprising:

loading into a memory ~~at least one~~ a first decryption key respectively associated with a first data frame including encrypted data, wherein said first decryption key is comprised of a first plurality of key values; and

reading out a second decryption key, the second decryption key comprises a second plurality of key values, for a second data frame, simultaneously with the step of loading ~~of the first plurality of~~ key values into the memory, wherein the step of reading out the second decryption key initiates a decryption operation using the key values for the second decryption keys already loaded into memory to decrypt said second data frame;

wherein the first decryption key and the second decryption key are different.

2. (Currently Amended) A method according to claim 1, said step of ~~initiating reading out a second the decryption operation key occurs simultaneously with loading of key values associated with subsequent data frames~~ further comprises initializing an S-box table with the key values for the second decryption key.

3. (Currently Amended) A method for executing an algorithm for encrypting data, comprising:

loading into a memory ~~at least one~~ a first encryption key respectively associated with a first data frame including unencrypted data, wherein each said first key is comprised of a first plurality of key values; and

reading out a second encryption key for a second data frame, the second encryption key comprising a second plurality of key values, simultaneously with the step of loading of first key values into the memory, wherein the step of reading out the second encryption key initiates an encryption operation using the second plurality of key values loaded into memory to encrypt said second frame;

Application No. 09/675,069
Response to Office Action dated 11/04/2004

wherein the first encryption key is different than the second encryption key.

Claims 4 - 24 (Canceled)

25. (New) A method for performing a decryption operation, comprising:
loading into a memory a first encryption key, the first encryption key comprising a first plurality of key values; and
reading the first plurality of key values to initialize a table before the loading step has completed.

26. (New) The method of claim 25, wherein the table is an S-box table.

27. (New) The method of claim 25, further comprising:
loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values with at least one of the second plurality of key values different than the first plurality of key values; and
wherein the loading into memory the second encryption key starts before the reading the first plurality of key values has completed.

28. (New) The method of claim 25, further comprising:
scrambling the table with the first encryption key; and
decrypting a first data packet using the scrambled table.

29. (New) The method of claim 28, further comprising:
loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values having at least one key value different than the first plurality of key values; and
wherein the loading into memory the second encryption key starts before at least one of the group consisting of scrambling the table and decrypting the first data packet has completed.

Application No. 09/675,069
Response to Office Action dated 11/04/2004

30. (New) A system for performing a decryption operation, comprising:
means for loading into a memory a first encryption key, the first encryption key comprising a first plurality of key values; and
means for reading the first plurality of key values to initialize a table responsive to start reading the first plurality of key values before the means for loading has completed loading the first plurality of key values.

31. (New) The method of claim 30, wherein the table is an S-box table.

32. (New) The method of claim 30, further comprising:
means for loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values with at least one of the second plurality of key values different than the first plurality of key values; and
wherein the means for loading into memory the second encryption key is responsive to start before the means for reading the first plurality of key values has completed.

33. (New) The method of claim 30, further comprising:
means for scrambling the table with the first encryption key; and
means for decrypting a first data packet using the scrambled table.

34. (New) The method of claim 33, further comprising:
means for loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values having at least one key value different than the first plurality of key values; and
wherein the means for loading into memory the second encryption key starts before at least one of the group consisting of means for scrambling the table and means for decrypting the first data packet has completed.

35. (New) A method for performing an encryption operation, comprising:

Application No. 09/675,069
Response to Office Action dated 11/04/2004

loading into a memory a first encryption key, the first encryption key comprising a first plurality of key values; and

reading the first plurality of key values to initialize a table before the loading step has completed.

36. (New) The method of claim 35, wherein the table is an S-box table.

37. (New) The method of claim 35, further comprising:

loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values with at least one of the second plurality of key values different than the first plurality of key values; and

wherein the loading into memory the second encryption key starts before the reading the first plurality of key values has completed.

38. (New) The method of claim 35, further comprising:

scrambling the table with the first encryption key; and
encrypting a first data packet using the scrambled table.

39. (New) The method of claim 38, further comprising:

loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values having at least one key value different than the first plurality of key values; and

wherein the loading into memory the second encryption key starts before at least one of the group consisting of scrambling the table and encrypting the first data packet has completed.

40. (New) A system for performing a decryption operation, comprising:

means for loading into a memory a first encryption key, the first encryption key comprising a first plurality of key values; and

Application No. 09/675,069

Response to Office Action dated 11/04/2004

means for reading the first plurality of key values to initialize a table responsive to start reading the first plurality of key values before the means for loading has completed loading the first plurality of key values.

41. (New) The method of claim 40, wherein the table is an S-box table.

42. (New) The method of claim 40, further comprising:

means for loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values with at least one of the second plurality of key values different than the first plurality of key values; and

wherein the means for loading into memory the second encryption key is responsive to start before the means for reading the first plurality of key values has completed.

43. (New) The method of claim 40, further comprising:

means for scrambling the table with the first encryption key; and
means for encrypting a first data packet using the scrambled table.

44. (New) The method of claim 43, further comprising:

means for loading into the memory a second encryption key, the second encryption key comprising a second plurality of key values having at least one key value different than the first plurality of key values; and

wherein the means for loading into memory the second encryption key starts before at least one of the group consisting of means for scrambling the table and means for decrypting the first data packet has completed.

45. (New) A method for performing encryption operations employing a dual ported memory, the dual ported memory comprising a read port and a write port, comprising:

reading out of the read port of the memory a first encryption key comprising a first plurality of key values for performing a first encryption operation; and

Application No. 09/675,069

Response to Office Action dated 11/04/2004

loading into write port of the memory a second encryption key for performing a second encryption operation, wherein the second encryption key is comprised of a second plurality of key values;

wherein the first decryption key and the second decryption key are different; and wherein the loading step starts before the reading step has completed.

46. (New) The method of claim 45, wherein the first encryption operation is encrypting a first data frame and the second encryption operation is decrypting a second data frame.

47. (New) A method according to claim 45, wherein the reading out of the read port comprises initializing an S-box table with the first plurality of key values.

48. (New) A method according to claim 47, wherein the reading out of the read port comprises scrambling the S-box table with the first encryption key after the initializing an S-box table has completed.

49. (New) A method according to claim 48, wherein the reading out of the read port comprises encrypting a data frame with the scrambled S-box table.

50. (New) A method according to claim 48, wherein the reading out of the read port comprises decrypting a data frame with the scrambled S-box table.